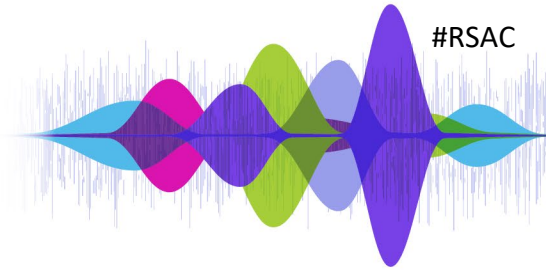
RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: MASH-W08

Green and Sustainable AI for Cybersecurity

Siân John MBE
Chief Technology Officer
NCC Group
https://www.linkedin.com/in/sian-john/



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

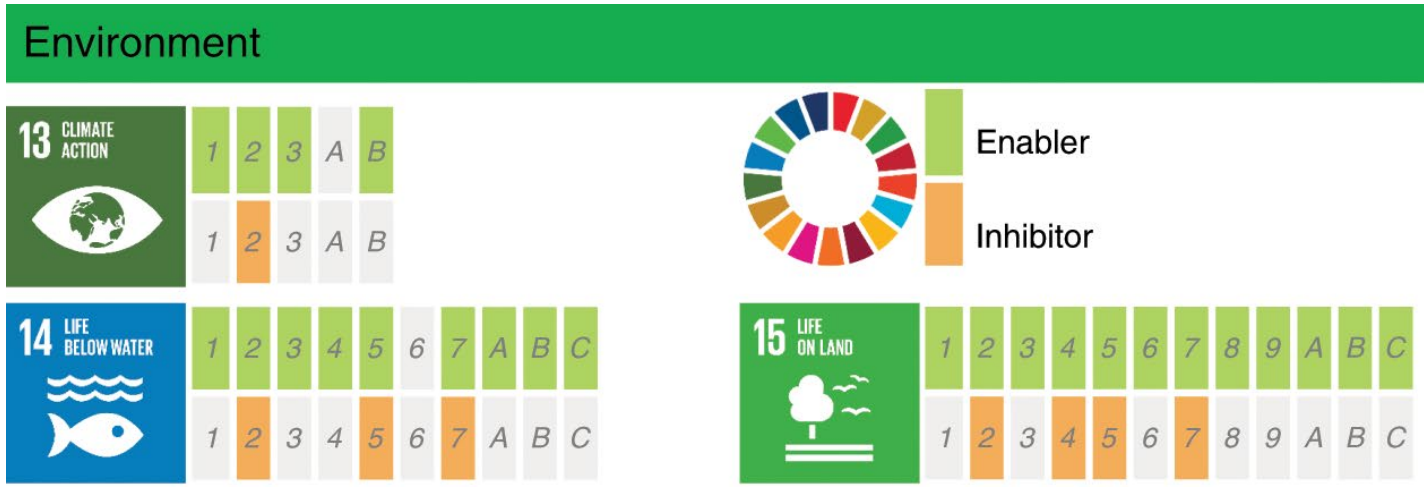
Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Thank you to Lesley Kipling at Microsoft for her contribution to and collaboration on this presentation.

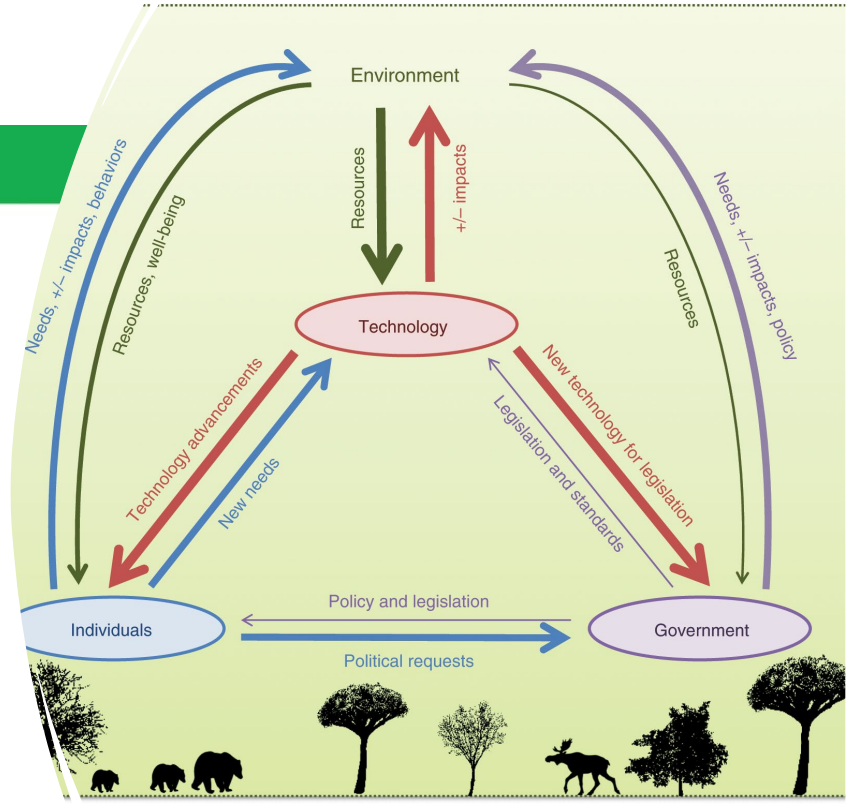
© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Technology and Society Interact

Brings Benefits but also Costs


Environment
13 CLIMATE ACTION
1 2 3 A B
1 2 3 A B
Enabler
Inhibitor
14 LIFE BELOW WATER
1 2 3 4 5 6 7 A B C
1 2 3 4 5 6 7 A B C
15 LIFE ON LAND
1 2 3 4 5 6 7 8 9 A B C
1 2 3 4 5 6 7 8 9 A B C

Source: [Nature Magazine: The role of artificial intelligence in achieving the Sustainable Development Goals]



Planetary boundaries

NetZero and Cybersecurity

Sustainable goal drives the push for renewable energy

Nation state threats target Critical National Infrastructure

Cyber Resilience is essential to **Sustainability**

Industrial Control Systems Cyber Challenges

Connecting Highly Complex and Sophisticated systems brings new risks

Not Secure by Design

Design restrictions do not support cyber security functions

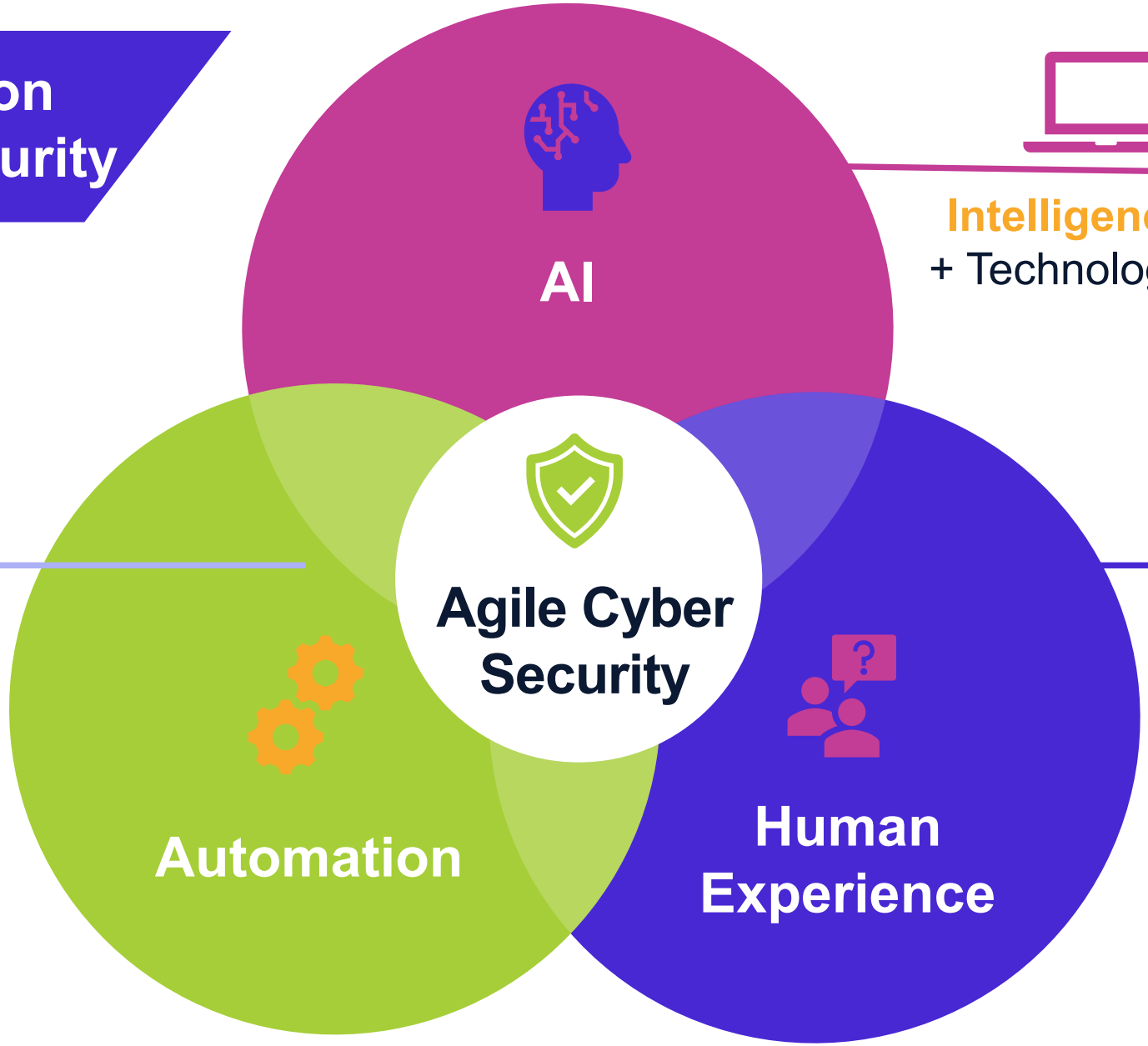
Air Gap “isolation” broken by technology advancements or vendor needs

Focus on availability makes comprehensive security checks difficult

Corporate IT security different to Industrial IT

Industrial IT/Energy Security needs Industrial Cyber Security

AI and Automation Key to Cybersecurity

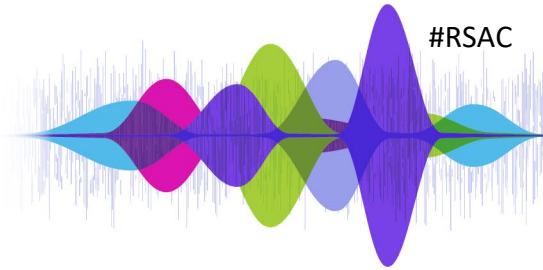


Intelligence
+ Technology

Innovation
+ Process

Insights
+ Context

AI/ML Used by Attackers and Defenders



… in Cyber Defence

- Machine Learning to detect malware
- Anti-Phishing and Deep Fake Detection
- Threat Intelligence and enrichment of detection data
- Detecting patterns and dealing with events at scale – “Minutes Matter”

… in Cyber Attack

- Adversarial Machine Learning to defeat detection software
- Improving Phishing Attacks and Deep Fakes for Social Engineering
- Detecting patterns and determining how to beat detection
- Scaling up attacks against infrastructure

Anomaly Detection: Network Intrusion

Early results with cuML RandomForest

- Sparse/Shallow forests vs. Dense/Deep
- Parameter tuning cuML RandomForest lead to:
  - Greater than 98% reduction in energy consumption
  - No accuracy trade-off *
- Reduced model complexity lowers energy consumption without sacrificing accuracy

Forest	Run-time (s)	$ Savings (% Delta)	E (Wh)	E Savings (% Delta)
Dense	4.99	0	54.2	0
Sparse	0.060	98.8	1.02	98.1

Source: https://github.com/danielgchen/MS_AZML_Anomaly_Detection

Dataset: KGG network intrusion subset

**All accuracy scores ≥ 0.9996, within ±0.03%*

Low priority GPU: NVIDIA T4 NC16as v3 @1.204/hr pay-as-you-go price

But AI also a Vulnerability

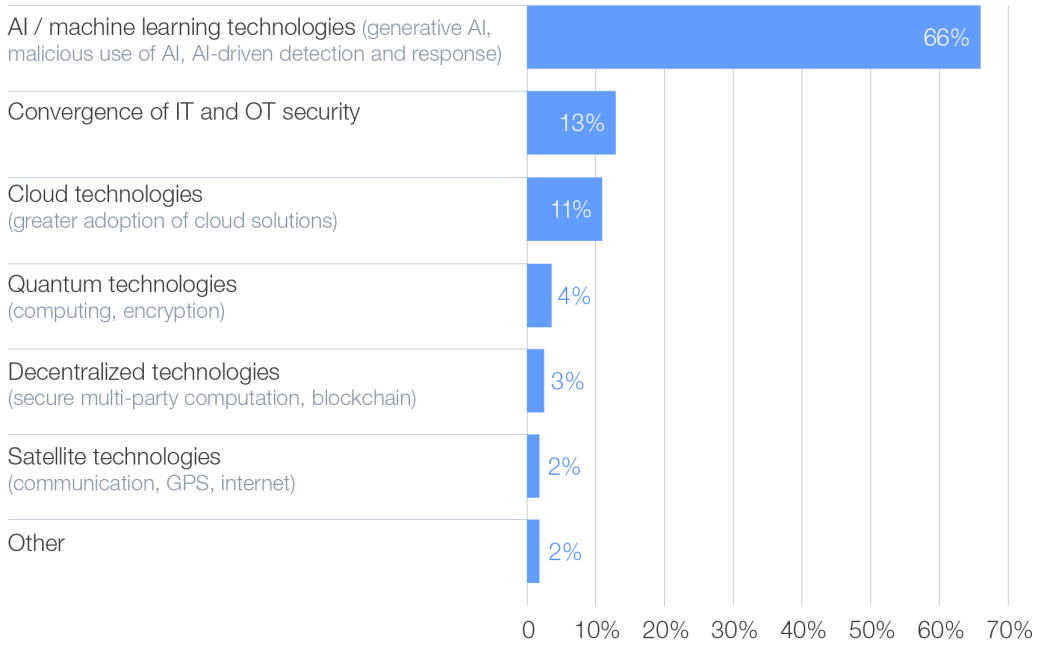
[Global Cybersecurity Outlook 2025 | World Economic Forum]

Global Cybersecurity Outlook 2025

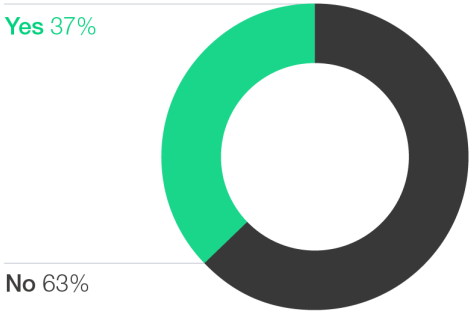
Cybersecurity vulnerabilities in 2025 predicted by professionals

WORLD ECONOMIC FORUM

In your view, which of the following will most significantly affect cybersecurity in the next 12 months?



Does your organization have a process in place to assess the security of AI tools before deploying them?



Framing

- GreenAI (*"Sustainable AI"*)
- Green *with* AI (*"Sustainability enabled by AI"*)

Do the **benefits** of a technology outweigh the **costs/impacts**?

- **Costs:** development (training), operation (inference), embodied carbon (hardware), storage (data)
- **Benefits:** AI used to accelerate decarbonization progress

Sustainability Definitions

Greenhouse Gas Emissions (GHG) measurement

Scope **1**

Direct emissions **created by your activities,**
like exhaust from company vehicles or diesel generators

Scope **2**

Indirect emissions **from the production of electricity or heat you use** to power buildings or processes

Scope **3**

Indirect value chain emissions **from all other activities in which you're engaged**, including all parts of your supply chain, from materials in buildings, business travel, and product lifecycle to the electricity your customers consume

Carbon targets

Carbon neutral: A company becomes carbon neutral by reducing their emissions and/or paying others to not emit an equivalent to their remaining emissions.

Carbon net zero: An organization is considered net zero carbon when it removes as much carbon as it emits.

Carbon negative: A company is carbon negative when it removes more carbon than it emits each year.

"meeting the needs of the present without compromising the ability of future generations to meet their own needs." - UN

Is AI a Low Carbon Technology Solution?

Professor Kate Crawford

"The energy difference from just doing a traditional search query to using a LLM is enormous"

"Some research indicates it can be up to 1,000 times more energy intensive."

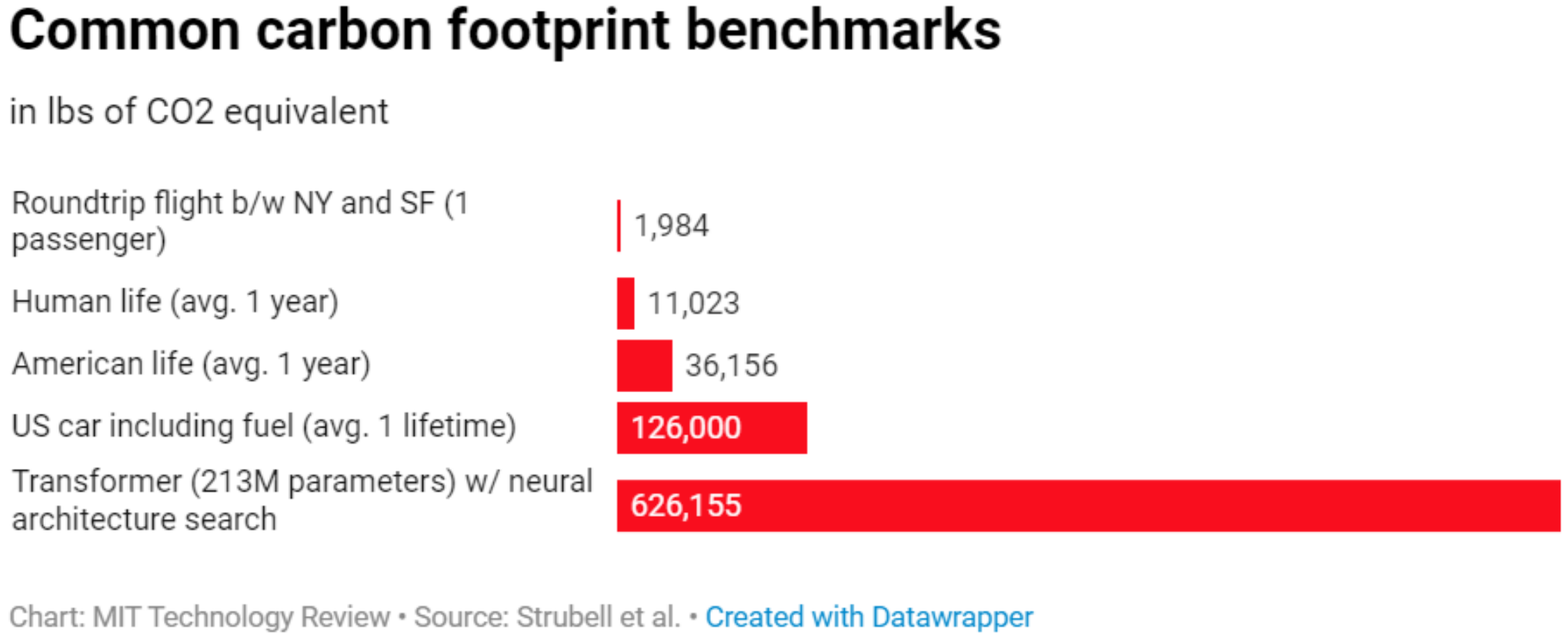
"All along the pipeline – the hardware, the software, the energy, the water to cool the systems – we have enormous environmental costs that are not being fully shared with the public."

Source: Kate Crawford: Exposing AI's costs | Baillie Gifford

"The question of the environmental cost of AI is the biggest secret in the industry right now"

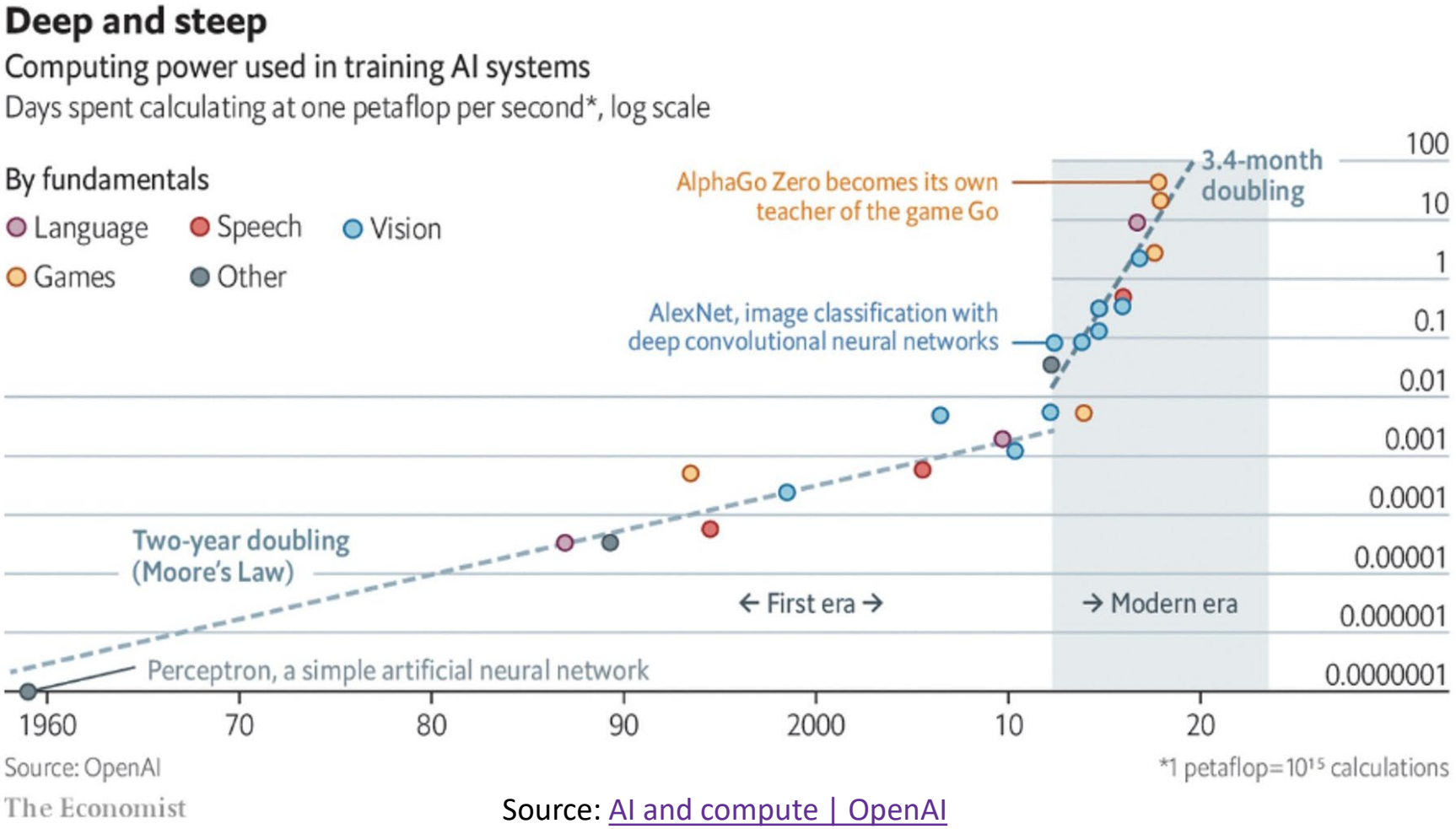
Source: Interview with Stephanie Hare at Bailie Gifford – October 2023

AI Carbon Costs

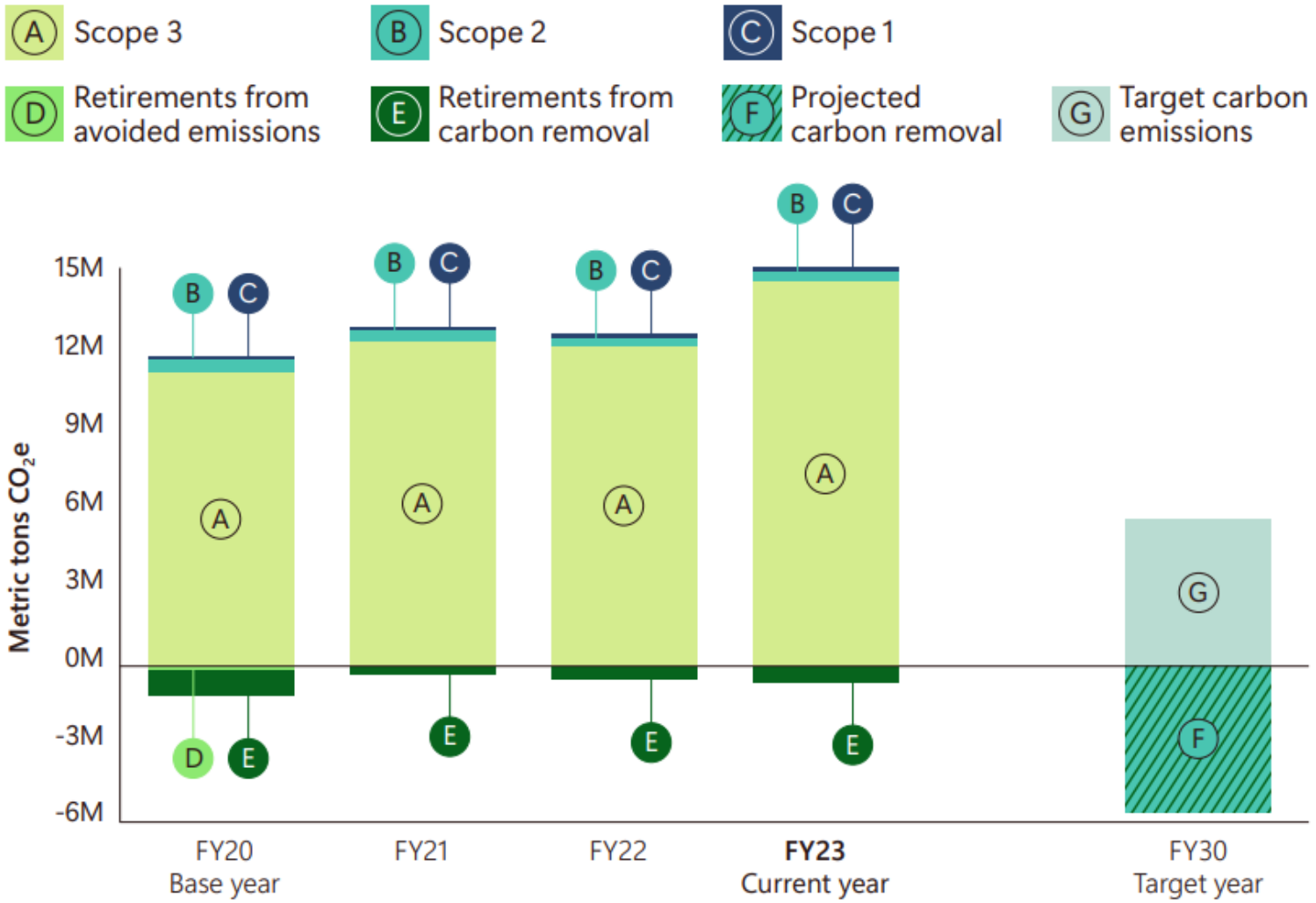

Common carbon footprint benchmarks
in lbs of CO2 equivalent
Roundtrip flight b/w NY and SF (1 passenger)
1,984
Human life (avg. 1 year)
11,023
American life (avg. 1 year)
36,156
US car including fuel (avg. 1 lifetime)
126,000
Transformer (213M parameters) w/ neural architecture search
626,155
Chart: MIT Technology Review • Source: Strubell et al. • Created with Datawrapper

Source: Training a single AI model can emit as much carbon as five cars in their lifetimes | MIT Technology Review

Assume Energy Consumption ~= Compute



Source: AI and compute | OpenAI



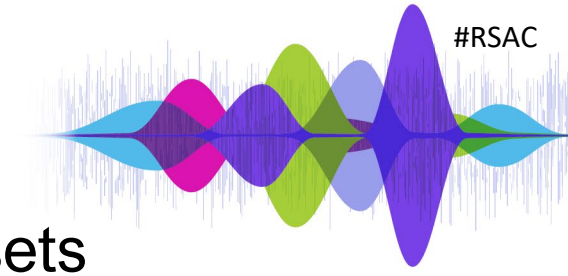
Microsoft Emissions increased by 29.1% in FY23

Scope 1
Direct emissions created by a company's activities

Scope 2
Indirect emissions from the consumption of the electricity or heat we use

Scope 3
Indirect emissions from all other activities in which we're engaged

Source: Microsoft Environmental Sustainability Report 2024



AI and Power

AI production pipeline

Build models by “training” on datasets

Derive predictions (“inferences”) by running models on new data points

Hardware and power needed

DL training requires specialized GPU hardware

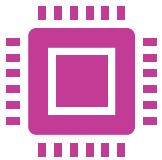
GPUs are power-hungry (often 250W-350W)

Inference may use GPUs, FPGAs, or CPUs (typical CPU ~135W, some up to 280W)

Source: https://devblogs.microsoft.com/sustainable-software/the-current-state-of-affairs-and-a-roadmap-for-effective-carbon-accounting-tooling-in-ai/

Microsoft Full-Stack Approach to Sustainable AI

Improving Energy Efficiency of AI



AI Optimization & Carbon Awareness

Silicon Innovation

Designing AI to do more with less

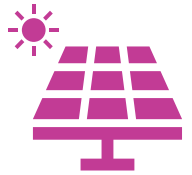
Advancing Low-Carbon Materials

Green Building Materials & Equipment

Supply Chain Decarbonization

Building low-impact supply chains

Optimizing Datacenter Energy and Water



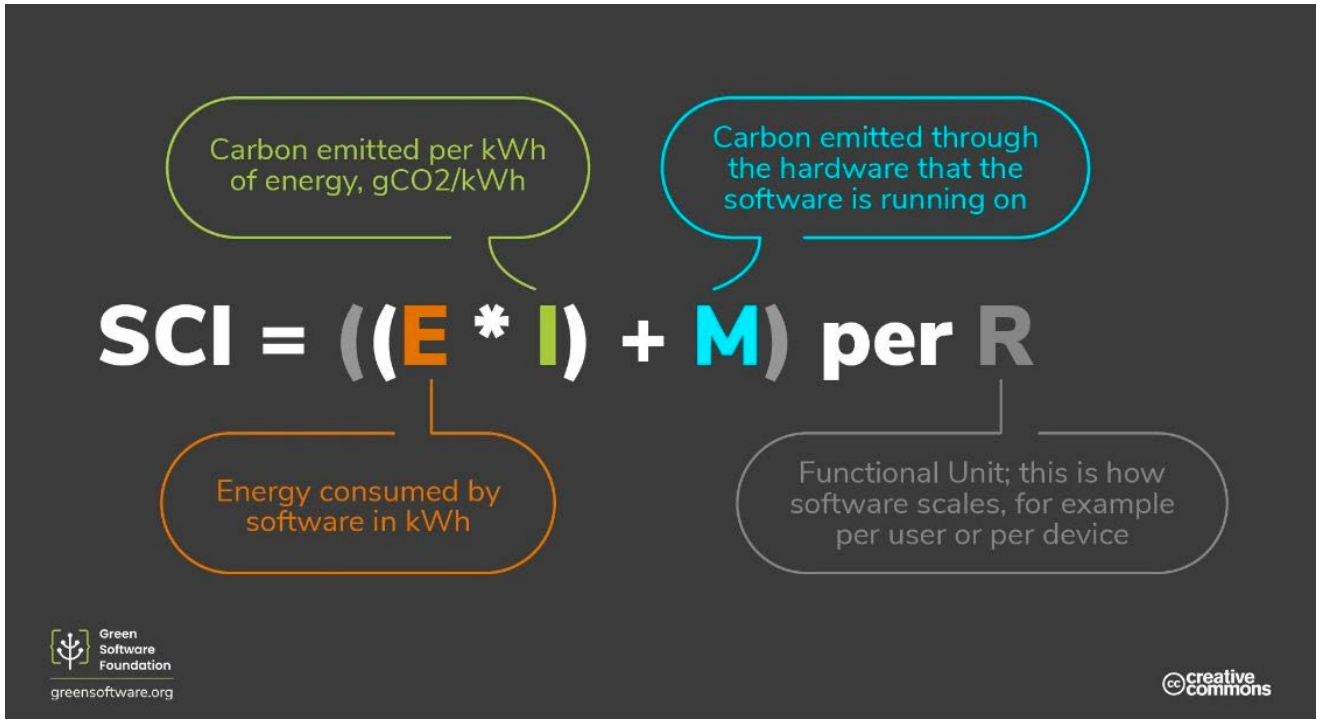
Carbon-Free Energy & Water-Free Operations

Carbon Removal and Water Replenishment

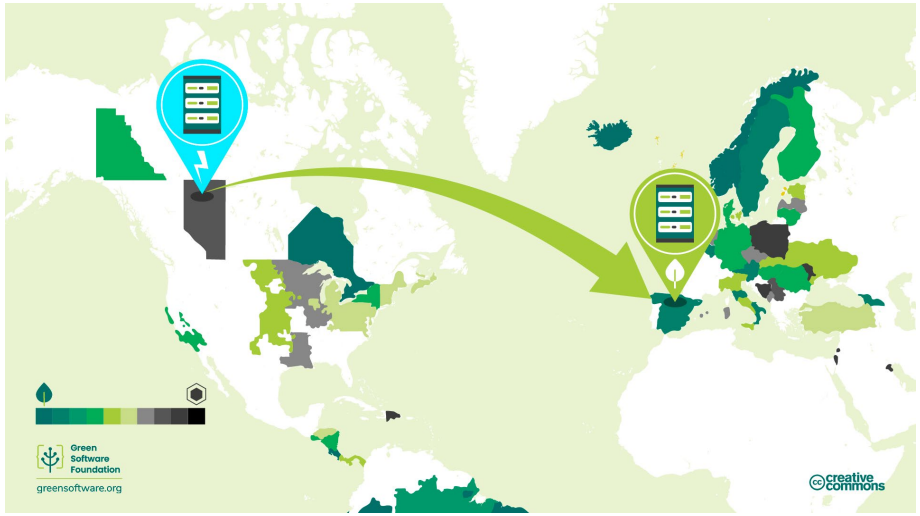
Operating to minimize & offset impact

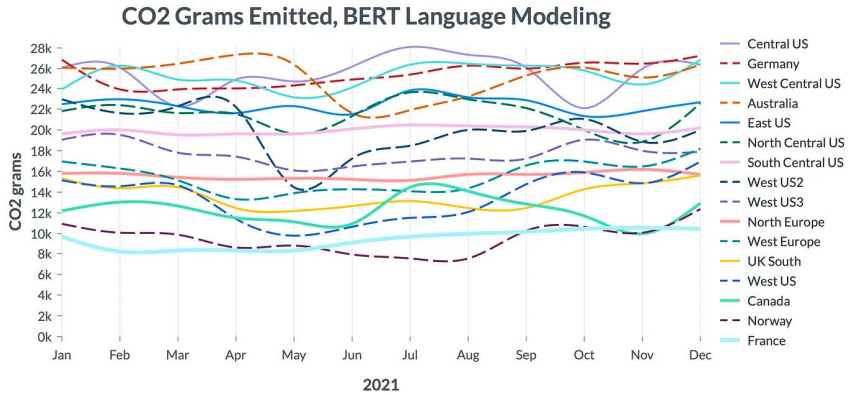
Reducing the Carbon Intensity of AI

- **Energy Efficiency (E):** make software use less electricity
- **Hardware Efficiency (M):** make software use fewer physical resources
- **Carbon Awareness (I):** adapt computation to take advantage of low carbon sources of electricity
  - Time shifting
  - Region shifting
  - Demand shaping


Carbon emitted per kWh of energy, gCO2/kWh
Carbon emitted through the hardware that the software is running on
SCI = ((E * I) + M) per R
Energy consumed by software in kWh
Functional Unit; this is how software scales, for example per user or per device
Green Software Foundation
greensoftware.org
creative commons

Example: Spatial Shifting | Region Selection





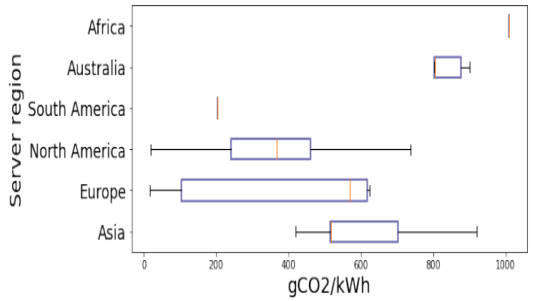
- Choosing the right location can reduce carbon by ~75%
- Must account for data transfer and data sovereignty
- **Greatest savings:** computational "bursts" with low data requirements

*A recent study shows almost **40X** difference within North America*

Quebec, Canda (20g CO2eq/kWh) vs.
Iowa, USA (736.6g CO2eq/kWh)

*Several studies have shown that these actions can result in a carbon reduction of as much as **45% to 99%***

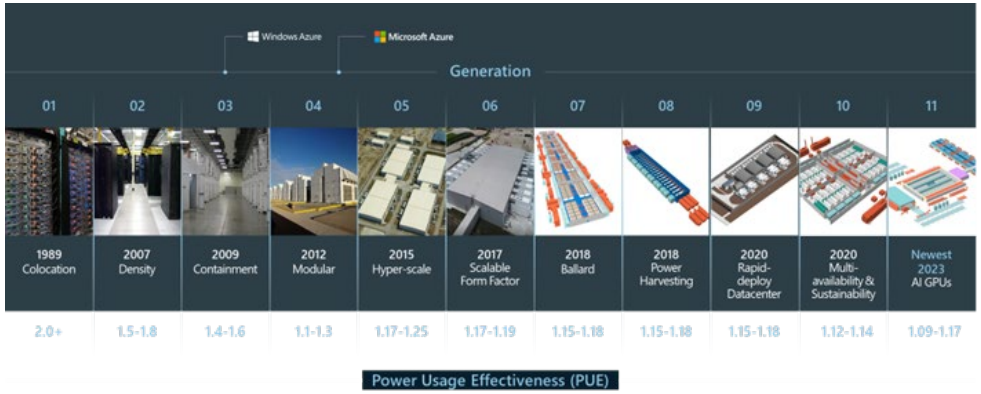
Emissions of 11 models

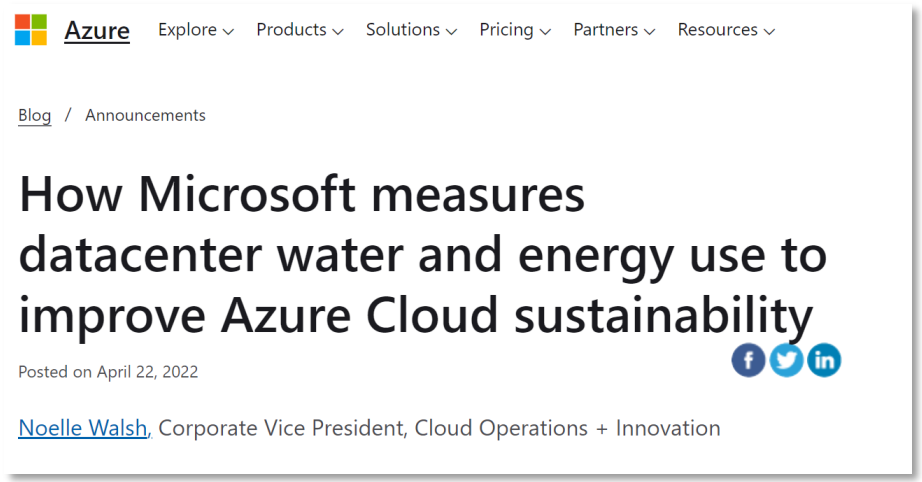


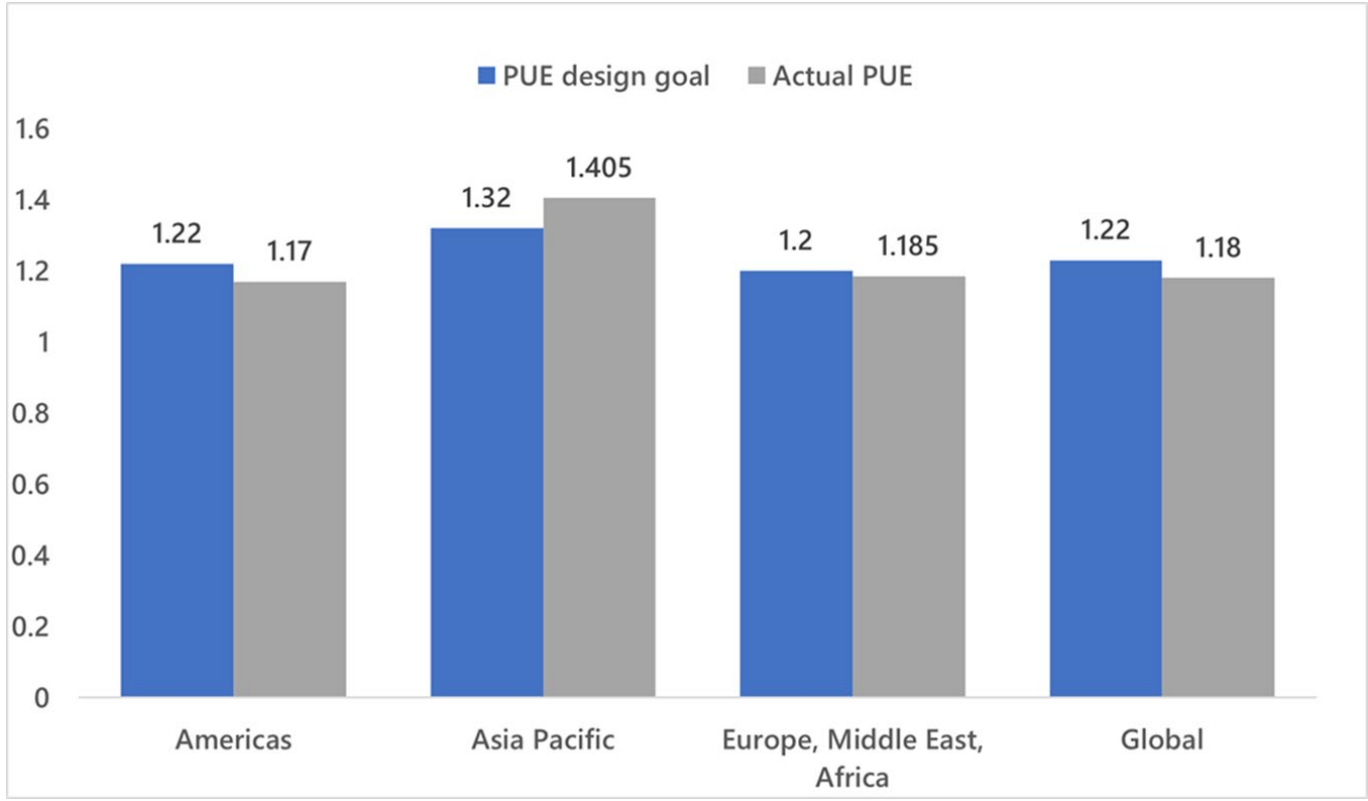
Source: https://learn.greensoftware.foundation/carbon-awareness

Building Sustainable Data Centres

Datacenter Energy Efficiency



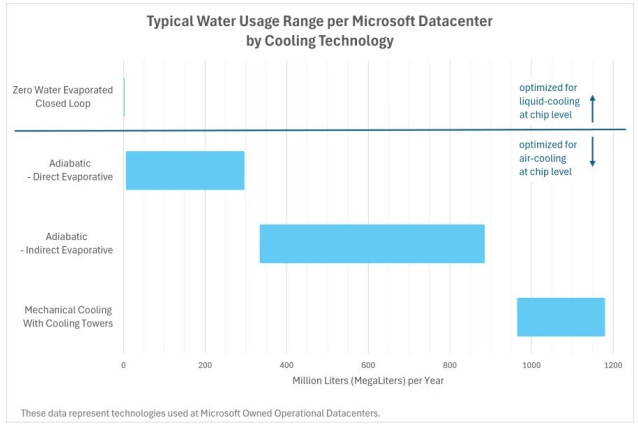


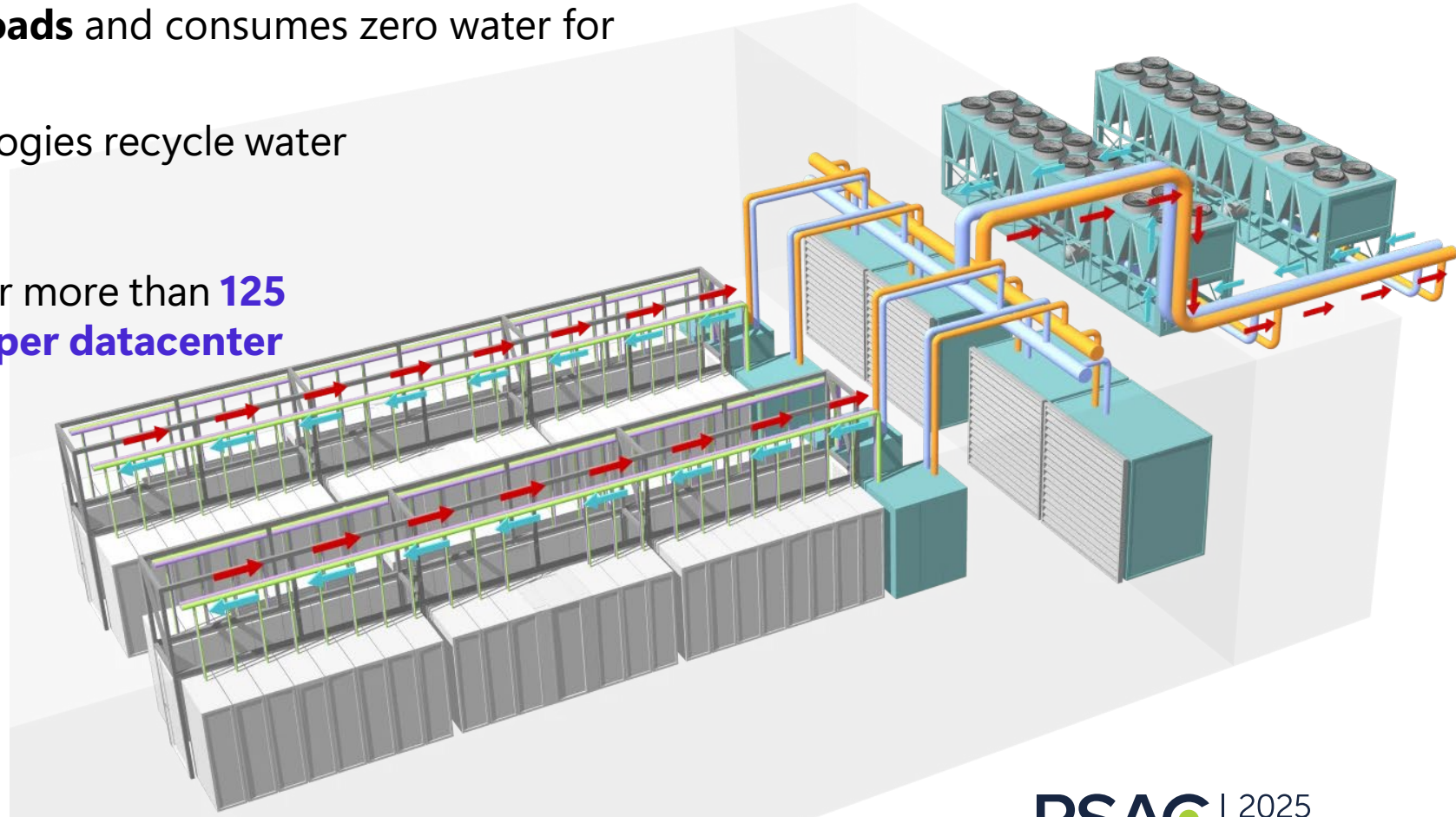


Source: How Microsoft measures datacenter water and energy use to improve Azure Cloud sustainability

Next-generation Datacenters Consume Zero Water for Cooling

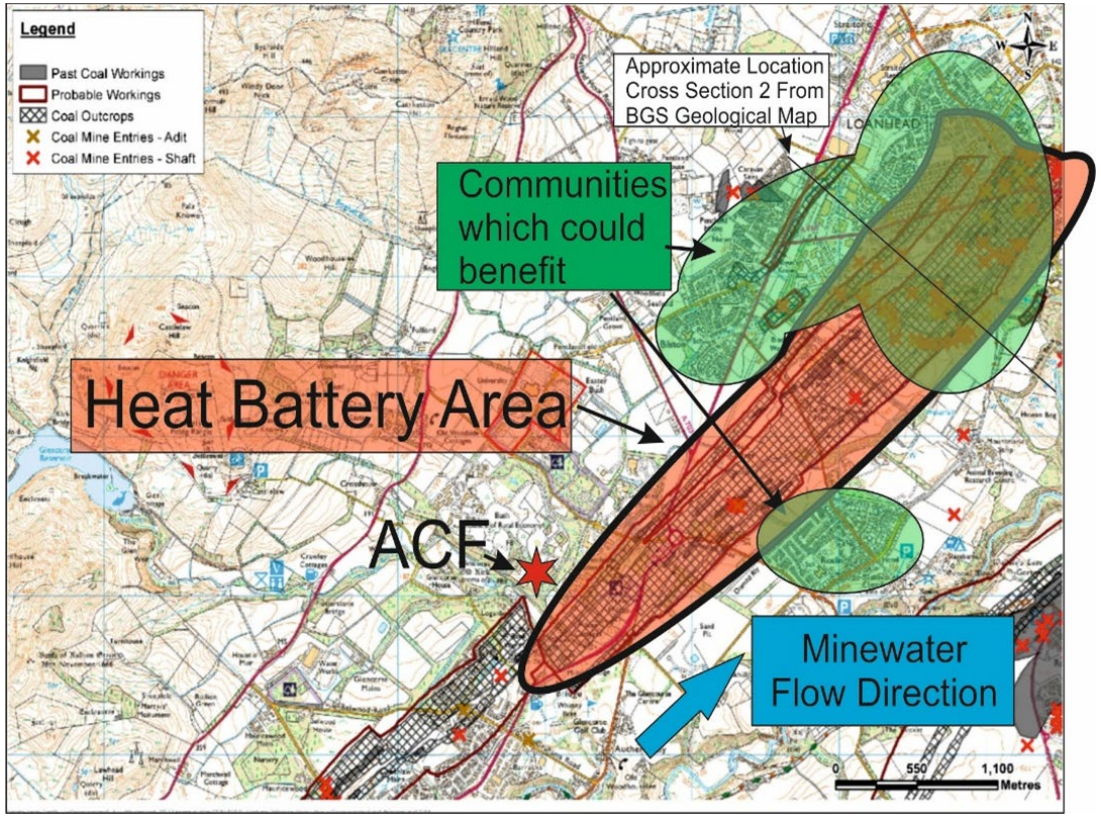
- Beginning in August 2024, Microsoft launched a new datacenter design that **optimizes AI workloads** and consumes zero water for cooling
- These new liquid cooling technologies recycle water through a closed loop.
- This design will avoid the need for more than **125 million liters of water per year per datacenter**

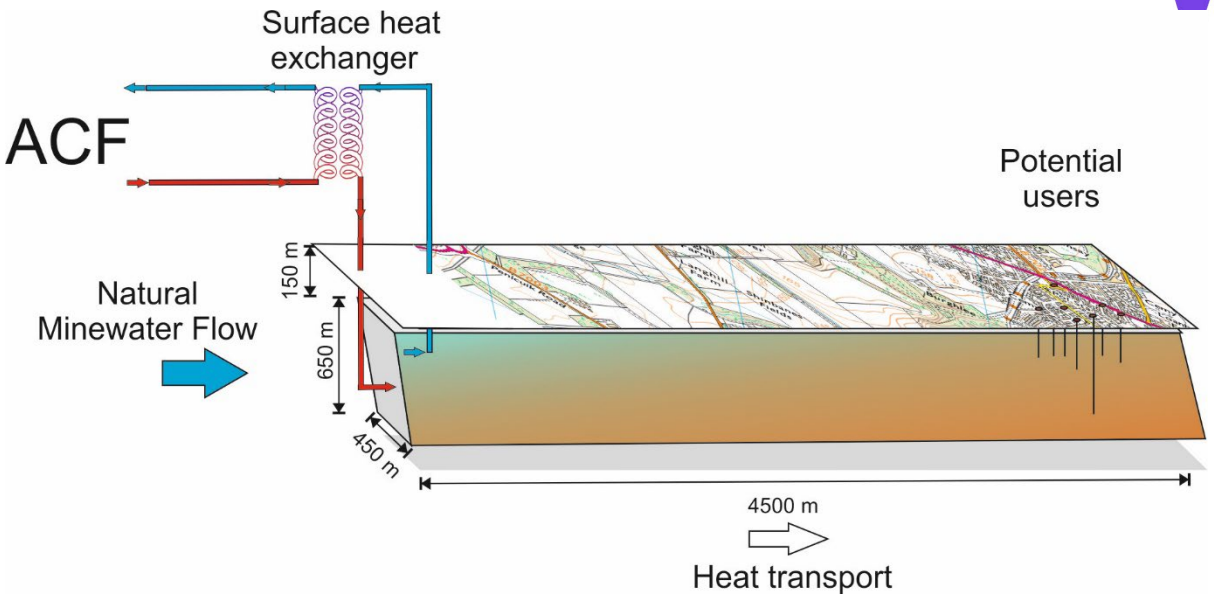




Heat Re-use Projects at the Edinburgh University ACF

- Two funded projects are underway
  1. Geobattery project to use local flooded mine workings to store heat – funded £2m+ proof of concept project with GeoSciences
  2. Connection of the Advanced Computing Facility hot water loops into the Easter Bush campus heating loop
- Cooling loop project in design stage
  - Higher output water temperatures make this project viable
  - Will use some, but by no means all, heat
  - Exascale expected to produce 14-15MW of heat in normal operation
  - Adjusting to reduce power consumption





- **Detailed feasibility study completed** to use hot water to heat abandoned mine workings
- Will create **geothermal heat battery** for use by homes, public and commercial buildings
- Water in mines **flows towards Edinburgh**
- Water used to **heat rocks** under south of city
- **Ground source heat pumps** extract heat from warmed rocks

- Funding secured to drill three **175m** deep boreholes
- **Extraction** point, **injection** point and **test** point
- Minewater temperature is **14C**

- **£2m project part-funded by Scottish Enterprise** to do detailed proof of concept over next 2 years

- Adjust clock speed to reduce consumption

Green Software Practitioner

Introduction | Learn Green Software

Green Software Practitioner

Take the exam | a Green Software Foundation project

- Welcome
- Introduction
- Carbon Efficiency
- Energy Efficiency
- Carbon Awareness
- Hardware Efficiency
- Measurement
- Climate Commitments
- Glossary

What is green software?

Green software is an emerging discipline at the intersection of climate science, software design, electricity markets, hardware, and data center design.

Green software is carbon-efficient software, meaning it emits the least carbon possible. Only three activities reduce the carbon emissions of software; energy efficiency, carbon awareness, and hardware efficiency. This training will explain all of these concepts, how to apply them to your processes and how to measure them, as well as some of the international guidelines and organizations that guide and monitor this space.

- What is green software?
- Who should read this?
- History
- How to be a green software practitioner
- Principles, Patterns, and Practices.

Green Software Principles

Energy Efficiency
Consume the least amount of electricity possible

Hardware Efficiency
Use the least amount of embodied carbon possible

Carbon Awareness
Do more when the electricity is clean and less when it's dirty

Green Software Foundation
greensoftware.org

creative commons

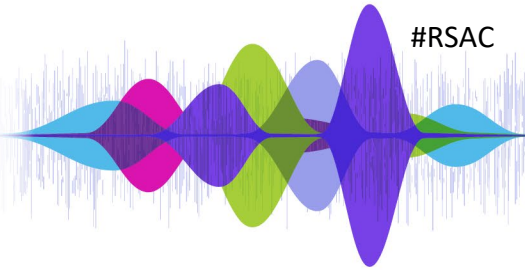
Cloud Native Applications

Using highly optimized managed services and platforms in the cloud enables cloud-native applications that inherently contribute to a better sustainability posture.

- Regular innovations in the service catalog
- Use the resources you need when you need it
  - Rightsizing
  - Disable out-of-hours workloads
  - Scaling patterns (vertical, horizontal, Autoscaling)
- Containerize workloads
- Event driven & Serverless architecture

Source: Application platform considerations for sustainable workloads on Azure - Microsoft Azure Well-Architected Framework | Microsoft Learn

Apply: Use the Right Tool for the Right Job

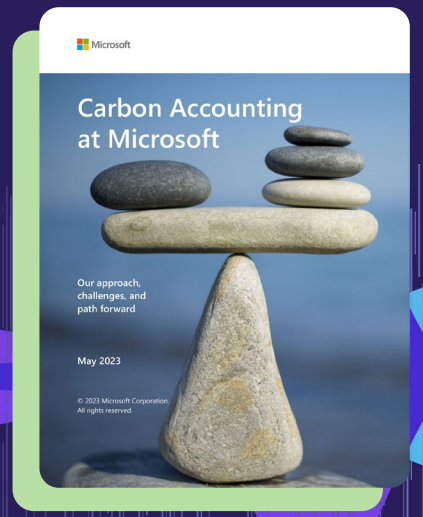


- Build solutions that are efficient and not overengineered, and so do what you want
- Look at where data is stored to be sustainable – data gravity! – not too deep iterations
- Think carefully about what you're using analytics for
- Don’t use generative AI / LLM models for things that an automation rule or script could possibly cover
- Cyber can’t survive without AI (e.g. machine learning rather than signatures for malware) but at the same time let’s use cyber to protect the infrastructure needed for Green AI.
- Ensure you/vendor has a secure and sustainable data centre design
- Ask your provider about how they train their models

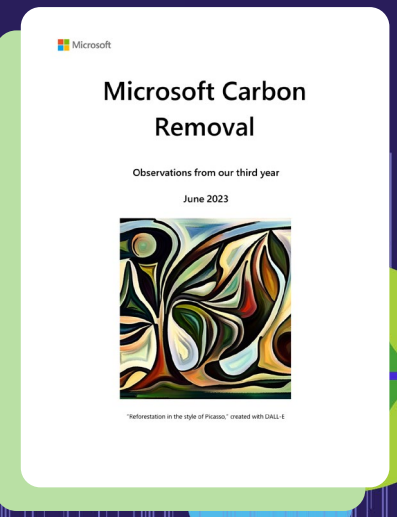
Sharing our learnings

ncc-group-plc-sustainability-report-2024.pdf

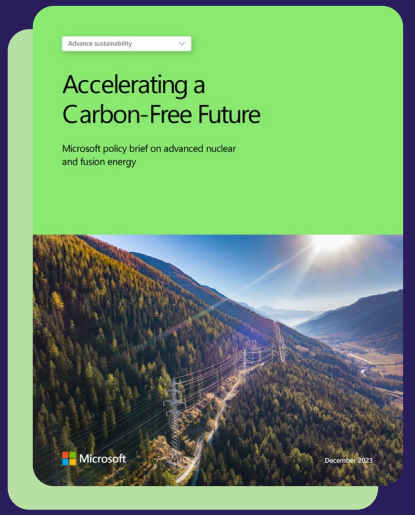
Accelerating sustainability with AI


Microsoft
Carbon Accounting at Microsoft
Our approach, challenges, and path forward
May 2023
© 2023 Microsoft Corporation. All rights reserved

Carbon Accounting at Microsoft

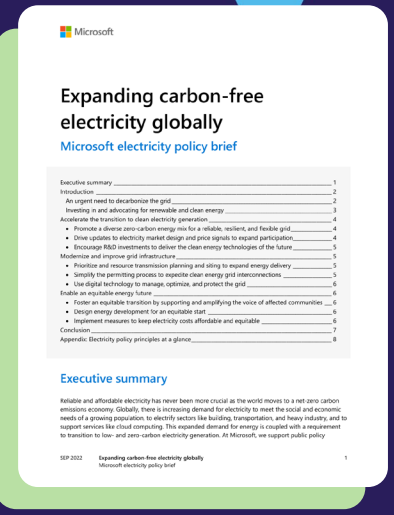

Microsoft
Microsoft Carbon Removal
Observations from our third year
June 2023
"Reforestation in the style of Picasso," created with DALL·E

Microsoft carbon Removal



Nuclear and fusion energy policy brief

Carbon policy brief



Electricity policy brief

nccgroup

Green and Sustainable AI,
Energy Resilient,
Cyber Resilient.

RSAC™ 2025 Conference

Many Voices.
One Community.

Thank you!!